WHAT IS CLAIMED IS:

1. A DNS server filter apparatus comprising:

packet verification means for verifying whether there is any abnormality in contents of a received DNS (domain name system) packet before transmitting it to a DNS server; and

error response means for generating an error response packet and transmitting it to a request source if an abnormality is detected.

2. A DNS server filter apparatus claimed in Claim 1:

wherein said packet verification means checks a DNS packet for obtaining information on a host name, a domain name, and an IP (Internet protocol) address transmitted from a network outside an organization by a person outside the organization using a DNS protocol; and

wherein said error response means generates an error response packet and transmits it to a request source when detecting an abnormality, thereby preventing the person outside the organization from invading a network of the organization by using private information of the organization and preventing the DNS server from operating abnormally by receiving a packet having an abnormal format.

3. A DNS server filter apparatus claimed in Claim 1:

wherein said packet verification means checks a DNS packet for obtaining information on a host name, a domain name, and an IP address transmitted to a DNS server belonging to a network outside the organization from a terminal inside the organization using the DNS protocol; and

wherein said error response means generates an error response packet and transmits it to a request source when detecting an abnormality, thereby preventing said DNS server belonging to the network outside the organization from operating abnormally.

4. A DNS server filter apparatus claimed in one of Claims 1 to 3, further comprising:

adding and deleting means for adding or deleting abnormality detecting conditions of the DNS packet.

5. A firewall apparatus wherein there is mounted said DNS server filer apparatus claimed in one of Claims 1 to 4.

6. A network system, further comprising:

a packet filtering firewall apparatus;

a DNS packet filter apparatus according to one of Claims 1 to 4 to communicate with the firewall apparatus; and

a DNS server for communicating with said DNS packet

filter apparatus.

7. A DNS server filter apparatus comprising:

a packet receiving section for receiving an inquiry from a terminal or a DNS server and a response packet from a DNS server;

a session management section for managing inquiry packets and response packets for an entire control, having a session management table for managing inquiry requests;

a packet verification section for verifying whether the inquiry packet or the response packet is abnormal;

a request generating section for generating an inquiry packet to the DNS server;

a response generating section for generating a response packet to be returned to a transmission source of the inquiry packet;

a packet transmitting section for transmitting the inquiry packet and the response packet; and

response means for verifying whether there is any abnormality in contents of the received packet in a DNS protocol before transmitting the packet to the DNS server regarding the received packet in the DNS protocol and generating an error response packet to transmit it to a request source if an abnormality is detected.

8. A DNS server filter apparatus claimed in Claim 7:

wherein said packet verification section comprises;

a calling management section for controlling operations of selecting and executing a verification program to be executed by referring to an attribute of said verification program, having a program management table containing entry point address information of the verification program, priority information of executing the verification program, and attribute information of the verification program;

a storage device in which the verification program is stored;

a load management section for loading an execution file of a verification program specified by a management tool or by a setting file on a memory, for initializing the loaded verification program, for registering an entry point of the verification program onto said program management table of said calling management section together with the obtained attribute, and for controlling a verification program specified to be deleted by said management tool so as to be released; and

a service routine comprising a subroutine group for utilizing functions of a DNS server filter body called by the executed verification program.

9. A DNS server filer apparatus claimed in Claim 8:

wherein said session management table comprises a pointer to a request packet, an IP address of a request

source which has issued an inquiry request, a port number of the request source which has issued the inquiry request, and a flag indicating whether the inquiry request has been transferred to another DNS server if the inquiry request has a normal packet format;

wherein said packet receiving section receives a DNS packet and then transmits the packet to said session management section; and

wherein said session management section makes settings of an IP address of a transmission source of the received packet, a port number of the received packet, and a flag value indicating "Testing" in said session management table, transmits the received packet to said packet verification section to request a packet verification, checks a type of said received packet to judge whether it is an inquiry request if there is any problem in contents of the verification as a result of the verification of said received packet in said packet verification section;

wherein if it is judged to be an inquiry request as a result of the judgement, the session management section requests said response generating section to generate an error response packet, requests said packet transmitting section to transmit the generated packet to a destination specified by the request source IP address and the request source port number on said session management table, and deletes information registered in said session management

table regarding the received packet to release the received inquiry request packet; and

wherein unless it is an inquiry request, the session management section searches said session management table to fetch a part related to an original inquiry request, requests said response generating section to generate an error response packet based upon an inquiry request packet by referring to the inquiry packet from the request packet pointer of an entry of said searched session management table, requests said packet transmitting section to transmit the generated response packet to a destination specified by the request source IP address and the request source port number on said session management table, deletes information registered in said session management table regarding the received response packet to release the response packet and deletes the entry registered in said session management table regarding the inquiry request corresponding to the response packet.

10. A DNS server filter apparatus claimed in Claim 9:

wherein said session management section checks a type of the received packet if there is no problem as a result of the packet verification performed in said packet verification section, searches said session management table for information on the inquiry request corresponding to the response packet if it is a response packet, and

verifies whether the received response packet can be a response to the original inquiry request;

wherein if there is a need for making an additional inquiry as a result of said verification, said session management section determines the next inquiry destination from the information of the received response packet, requests said request generating section to generate an inquiry request packet, requests said packet transmitting section to transmit it to the next inquiry destination, and deletes information on the response packet in progress of the received inquiry from said session management table to release the response packet; and

wherein if the received response packet can be a response to the original inquiry request packet as a result of said verification, the session management section requests said response generating section to generate a response packet to the original inquiry request reflecting the result of the response packet of receiving the response packet, requests said packet transmitting section to transmit it to the transmission source of the original inquiry request, deletes information related to the received response packet from said session management table, and deletes information related to the original inquiry request from said session management table to release the response packet.

11. A DNS server filter apparatus claimed in Claim

9 or 10:

wherein said session management section checks a type of the received packet if there is no problem as a result of the packet verification in said packet verification section, checks a transmission source of the received packet if the received packet is an inquiry request and then unless said transmission source is a network inside an organization issuing an inquiry, determines a DNS server outside the organization to which an inquiry is issued first to meet the inquiry request of a network outside the organization, requests said request generating section to generate an inquiry request based upon the original inquiry request, and requests said packet transmitting section to transmit the inquiry to said determined DNS server, or if said transmission source is the network inside the organization issuing the inquiry, requests said request generating section to generate an inquiry request packet base upon the received inquiry request packet, requests said packet transmitting section to transmit the inquiry packet to the DNS server, sets a "Inquiring" value to the flag among the entries of said session management table corresponding to the received packet, and sets a pointer to the received packet to the pointer of the entry on said session management table.

12. A DNS server filter apparatus claimed in Claim 7, wherein a cache memory previously stores DNS server

information.

13. A record medium having a program recorded therein and capable of executing:

packet receiving processing for receiving an inquiry from a terminal or a DNS server in the DNS protocol and a response packet from a DNS server via a communication apparatus;

session management processing for managing inquiries and response packets for an entire control, having a session management table for managing the inquiry requests;

packet verification processing for verifying whether an inquiry or a response packet is abnormal;

request generation processing for generating an inquiry packet to a DNS server;

response generation processing for generating an inquiry packet to the DNS server;

response generation processing for generating a response packet to be returned to a transmission source of the inquiry packet;

packet transmission processing for controlling an operation so as to transmit an inquiry and a response packet through a communication apparatus; and

DNS server filter processing for verifying whether there is any abnormality in contents of the packet before transmitting the packet to the DNS server regarding the

received DNS packet; if an abnormality is detected, it generates and transmits an error response packet.

14. A record medium claimed in Claim 13, having a program recorded therein and capable of executing:

wherein said program management table comprises entry point address information of the verification program, priority information of executing the verification program, and attribute information of the verification program;

wherein the calling management processing is performed for selecting and executing a verification program to be executed by referring to the attribute of said verification software; and

wherein the load management processing is performed for loading an execution file of the verification program specified by a management tool or a setting file on a memory, for initializing the loaded verification program, for registering an entry point of the verification program together with an obtained attribute on said program management table, and for releasing a verification program specified to be deleted by said management tool from the memory.

15. A group of recording media, wherein said program claimed in Claim 13 is divided into a plurality of portions and said portions are recorded on said media,

respectively.

16. A group of recording media, wherein said program claimed in Claim 14 is divided into a plurality of portions and said portions are recorded on said media, respectively.

17. A program embodied as electric signals, comprising:

packet receiving processing for receiving an inquiry from a terminal or a DNS server in the DNS protocol and a response packet from the DNS server via a communication apparatus;

session management processing for managing the inquiry and the response packet for an entire control using a session management table for managing inquiry requests;

packet verification processing for verifying whether the inquiry and the response packet are abnormal;

request generation processing for generating an inquiry packet to the DNS server;

response generation processing for generating a response packet returned to a transmission source of the inquiry packet;

packet transmission processing for controlling an operation to transmit the inquiry and the response packet via the communication apparatus; and

DNS server filter processing for verifying whether there is any abnormality in contents of the received DNS packet before transmitting the packet to the DNS server regarding the received DNS packet and for generating and transmitting an error response packet when detecting an abnormality.

18. A program claimed in Claim 17 embodied as electric signals, further comprising:

a program management table having entry point address information of the verification program, priority information for executing the verification program, and attribute information of the verification program,

calling management processing for selecting and executing a verification program to be executed by referring to the attribute of said verification software; and

load management processing for loading an execution file of the verification program specified by a management tool or a setting file on a memory, for initializing the loaded verification program, for registering an entry point of the verification program together with the obtained attribute on said program management table, and for releasing the verification program specified to be deleted by said management tool from the memory.